



## HPE StoreEver MSL3040/6480 Tape Library

KeyControl® Integration Guide

© 2025 Entrust Corporation. All rights reserved.

## Table of Contents

1. Introduction	1
1.1. Product configurations	1
1.2. Requirements	1
2. Deploy and configure KeyControl	2
2.1. Deploy a KeyControl cluster	2
2.2. Additional KeyControl cluster configuration	2
2.3. Configure authentication	3
2.4. Create DNS record for the KeyControl cluster	3
2.5. Create a KMIP Vault in the KeyControl	3
2.6. View the KMIP Vault details	7
3. Integrate KeyControl with StoreEver	9
3.1. Obtain the CA certificate	9
3.2. Configure the KMIP server.	9
3.3. Create the client certificate bundle	. 11
3.4. Import tenant client certificate into the StoreEver Tape Library	. 13
3.5. Set the default encryption mode	. 15
4. Test the integration.	. 16
5. Integrating with an HSM	. 21
6. Additional resources and related products	22
6.1. Entrust products	22
6.2. nShield product documentation	22

## Chapter 1. Introduction

This document describes the integration of the Hewlett Packard Enterprise (HPE) StoreEver MSL3040/6480 Tape Library (referred to as StoreEver in this guide) with the Entrust KeyControl key management solution using the open standard KMIP protocol. KeyControl serves as a key manager for encryption keys by using various protocols, including KMIP.

## 1.1. Product configurations

Entrust has successfully tested the integration of KeyControl with HPE StoreEver MSL3040/6480 Tape Library in the following configurations:

System	Version
Entrust KeyControl	10.2

## 1.2. Requirements

Before starting the integration process, familiarize yourself with:

- HPE StoreEver MSL3040 Tape Library User and Service Guide
- HPE StoreEver MSL6480 Tape Library User and Service Guide
- Entrust KeyControl Online Documentation Set

## Chapter 2. Deploy and configure KeyControl

## 2.1. Deploy a KeyControl cluster

For the purpose of this integration, a two-node cluster was deployed as follows:

- 1. Download the KeyControl software from Entrust TrustedCare. This software is available as an OVA or ISO image. This guide deploys an OVA installation.
- 2. Install KeyControl as described in KeyControl OVA Installation.
- 3. Configure the first KeyControl node as described in Configuring the First KeyControl Node (OVA Install).
- 4. Add second KeyControl node to cluster as described in Adding a New KeyControl Node to an Existing Cluster (OVA Install).



Both nodes need access to an NTP server, otherwise the above operation will fail. Sign in to the console to change the default NTP server if required.

<b>ENTRUST</b>	KeyControl Vault Management			DG ALERTS	SETTINGS	🛓 Security Administrator 👻 🛛 🖁	winch то: Nanage Vaults <b>?</b>
Actions - Cluster Servers Multi-Select C Refresh					Select $\Box$ Refresh ${\cal G}$		
Node 👻	Status 🗸	Server Name				Y IP Address	~ =
🔒 Current Node	Online	🗙 AN TOMO I DAN FAMIL					^
	Online	ALCORD DOLLARS					
Name							~
Name.		Continue (					
status:		Unine					
Authenticated:		Yes					
Domain:		Appliance Management A	dmin Group				
IP Address:							
Certificate:		Internal Web server: Defa External Web server: Defa	ult ault				

5. Install the KeyControl license as described in Managing the KeyControl License.

## 2.2. Additional KeyControl cluster configuration

After the KeyControl cluster is deployed, additional system configuration can be done as described in KeyControl System Configuration.

## 2.3. Configure authentication

This guide uses local account authentication.

For AD-managed Security groups, configure the LDAP/AD Authentication Server as described in Specifying an LDAP/AD Authentication Server.

## 2.4. Create DNS record for the KeyControl cluster

This guide uses the individual IP addresses of the KeyControl nodes.

To use hostnames, configure your DNS server giving each node in the KeyControl a unique name.

## 2.5. Create a KMIP Vault in the KeyControl

The KeyControl Vault appliance supports different type of vaults. For example: cloud key management, KMIP, PASM, database, and others. This section describes how to create a KMIP vault for tis integration.

Refer to the Creating a Vault section of the admin guide for more details.

- 1. Sign in to the KeyControl Vault Server web user interface:
  - a. Use your browser to access the IP address of the server.
  - b. Sign in using the **secroot** credentials.
- 2. From the user's dropdown menu, select Vault Management.



3. In the KeyControl Vault Management interface, select Create Vault.

ENTRUST KeyControl Vault Management	ی secroot ب Switch to: Applicance Management ?
Vaults Each vault has unique authentication and management	🖨 Settings
+	
Let's get started!	
+ Create Vault	

4. In the Create Vault page, select KMIP. Then enter your information.

For example: Create Vault A vault will have unique authentication and management. Туре Choose the type of vault to create KMIP ~ Name\* HPE-StoreEver-MSL3040-MSL6480 Description HPE StoreEver MSL 3040/6480 integration with Entrust KeyControl Max. 300 characters Administration Invite an individual to have complete access and control over this vault. They will be responsible for inviting additional members. Admin Name\* Administrator Admin Email\* **Create Vault** Cancel

5. Select Create Vault, then select Close.

A window with the newly created vault information appears. In addition, an email with

the same vault information is sent to the security administrator **secroot**.

Example vault information window:

#### Vault Successfully Created

You will need to send the following information to the Vault Admin so they can log into their vault

Vault URL Copy User Name Administrator@hpe.com Copy Temporary Password Close

Example email:

<b>ENTRUST</b>	KeyControl
Administrator, you have bee vault, CommVault.	en invited to become an administrator of the KMIP
To sign in, use the following:	
URL:	
User Name:	
Password:	
If you have any issues, <u>contact support</u> .	
©2023 Entrust Corporation. All Rights Reserved	1

6. Bookmark the **Vault URL** listed above.

The newly created Vault is added to the **Vault Management** dashboard.

For example:

ENTRUST KeyControl Vault Management	secroot v SMITCH TO: Appliance Management
Veults Each vault has unique authentication and management	Settings
Total Vaults: 2	+ Create Vault
КМІР	
HPE-StoreEver-MSL304 0-MSL6480	
HPE StoreEver MSL3040/6480 Integra tion with Entrust KeyControl	

7. Sign in to the **Vault URL** with the temporary password. Change the initial password when prompted. Sign in again to verify.

For example:



#### KeyControl Vault for KMIP

Sign in to your account

S)

8. Notice the new vault.

For example:

## 2.6. View the KMIP Vault details

1. Hover over the Vault and select **View Details**.

For example:

### Vault Details

 $\times$ 

#### HPE-StoreEver-MSL3040-MSL6480

HPE StoreEver MSL3040/6480 integration with Entrust KeyControl

#### Туре

KMIP

#### Created

Jun 13, 2024 10:28:41 AM

Vault URL

6.000/

🖪 Сору

API URL

High J. 10.12.12.2012/Investig Tenants/1024. coginy/MCMSRCs (2017) - Build BERRS STRUCTURE STRUCTURE

🖪 Сору

#### Administrator

Admin Name Administrator

#### User Name

A development of the group of the second

Close

2. Select **Close** when done.

# Chapter 3. Integrate KeyControl with StoreEver

Follow these steps to register Entrust KeyControl as a KMS in HPE StoreEver Tape Library.

- 1. Obtain the CA certificate
- 2. Configure the KMIP server
- 3. Create the client certificate bundle
- 4. Import tenant client certificate into the StoreEver Tape Library
- 5. Set the default encryption mode

## 3.1. Obtain the CA certificate

The Entrust KeyControl KMIP server can accept a certificate from your local root CA or a trusted CA, or can act as local root CA itself. For the purpose of this integration the Entrust KeyControl KMIP server will act as the local root CA. Execute the following steps to obtain the local root CA certificate for the Entrust KeyControl KMIP server.

- 1. Sign in to the KMIP Vault with the URL and credentials from Create a KMIP Vault in the Entrust KeyControl.
- 2. Go to the Vault Management window by selecting SWITCH TO Manage Vaults / SWITCH TO Appliance Management in the top right corner of the window.
- 3. Select the ? icon in the top right corner of the window, then select **Download CA** certificate.
- 4. Save the certificate for later use. Example filename: 240614140352\_cacert.pem.

## 3.2. Configure the KMIP server

- 1. Log into the StoreEver webGUI using an account with Security Admin privileges.
- 2. Select the **Configuration** box.
- 3. Expand the Encryption menu in the right toolbar, then select KMIP Wizard.

Key Management Interoperability Protocol (KMIP) Wizard	Wizard Information
Wizard Information     Certificate Authority Information     Certificate Authority Certificate Entry	With the KMIP Wizard you can configure the library for use with the KMIP key management server. Before starting the wizard, ensure that the library configuration is complete, including defining all library partitions. Also, ensure that the KMIP server has been put on the network and configured for use with this library. For questions on the KMIP server setup, see the applicable KMIP server user guide.
Library Certificate Information	To continue the wizard, click Next.
KMIP Client Configuration	To clear the wizard settings when no longer using this encryption method or reset the wizard configuration to its default
Certificate Generation	state, click Qear An Wizard Settinga.
Sign Library Certificate	Clear All Wizard Settings
KMIP Server Configuration	
Setup Summary	
Hewlett Packard Enterprise	Back Next Finish Cancel

- 4. Select Clear All Wizard Settings to remove any prior configuration.
- 5. Select Next twice.
- In the Certificate Authority Certificate Entry window, copy-paste the certificate from section Obtain the CA certificate into the Certificate Authority (CA): text box, then select Next.

Key Management Interoperability Protocol (KMIP) Wizard	Certificate Authority Certificate Entry
	Retrieve the local Certificate Authority's (CA) certificate.
Wizard Information	Within the KMIP Management Console:
Certificate Authority Information	1. From the KMIP server, locate the CA certificate that you have chosen to use.
Certificate Authority Certificate Entry	2. Copy the certificate text.
,	Be sure to include the "BEGIN CERTIFICATE" and " END CERTIFICATE" lines in your selection. 3. Please pasts the certificate of the signing authority below.
Library Certificate Information	<ol> <li>Heade paster meter metare of metargining admontly below.</li> <li>A. Click Next</li> </ol>
KMIP Client Configuration	Certificate Authority (CA):
Certificate Generation	BEGIN CERTIFICATE REQUEST
Sign Library Certificate	Consequences of the second s
KMIP Server Configuration	
Setup Summary	and the second
	11 Summarian Conjugate AL / Stamport and reacting and a reacting month of the second
	Annual Spatter dual Prace public Calledon dual Callpaners du Denance Calledon d'Annual general de result renan
	· · · · · · · · · · · · · · · · · · ·
	//////////////////////////////////////
Hewlett Packard Enterprise	Back Next Finish Cancel

- 7. Select Next twice.
- 8. In the KMIP Client Configuration Window, check Enable KMIP Certificate-only authentication, then select Next.



- 9. In the **Certificate Generation** window, select the **Generate New Certificate** radio button.
- 10. When certificate request has been generated, copy the certificate request to a file, for example, hpe-storeever-3040.csr, then select **Next**.

Key Management Interoperability Protocol (KMIP) Wizard	Certificate Generation
	Keep Current Certificate
Wizard Information	O Generate New Certificate
Certificate Authority Information	Generate a certificate that is later signed for use on library.
	Copy the entire certificate.
Certificate Authority Certificate Entry	NOTE: Besure to include the
Library Certificate Information	"BEGIN CERTIFICATE" and "END CERTIFICATE" lines in your selection
	When you have copied the certificate, click Next
KMIP Client Configuration	
► Certificate Generation	Library Certificate Select Certificate
Sign Library Certificate	
KMIP Server Configuration	
	APTOR 71, No. 2 File in participant of the APT and the Later of the United States and the
Setup Summary	Productive Country geogenetics on American Country and Country for Country for Country for Country and
	genter anderer i seet konne griet i 191 oande frittene als gefrittet i 191 oak e traditieren.
	A second s
Hewlett Packard	
Enterprise	Back Next Finish Cancel

11. Pause configuring the KMIP server. You will continue further down.

## 3.3. Create the client certificate bundle

1. Sign in to the KMIP Vault with the URL and credentials from section Create a KMIP

#### Vault in the Entrust KeyControl.

2. Select Security, then Client Certificates.



- 3. In the **Manage Client Certificate** page, select the **+** icon on the right to create a new certificate. The **Create Client Certificate** dialog box appears.
- 4. In the Create Client Certificate dialog box:
  - a. Enter the **Certificate Name**.
  - b. Select the Certificate Expiration.
  - c. Upload the certificate request created in section Configure the KMIP server.
  - d. Select Create.

For example:

Create Client Certificate		×
Add Authentication for Certificate		
Certificate Name *		
HPEStoreEver3040		
Certificate Expiration *		
Jun 14, 2025		
Certificate Signing Request (CSR)		
hpe-storeever-3040.csr		Browse
Encrypt Certificate Bundle		
	Cancel	Create

The new certificates are added to the Manage Client Certificate pane.

۱	ENTRUST KeyCont	rol (MIP		HPE-Store MSI 6480	Ever-MSL3040-	¢	4	?
🕌 Ho	me 🔹 Client Certificates 🛛 🛪							
Mana	ge Client Certificate							
Filter					止 Downl	load	+	Û
	Name	Valid From	Expiration	Generated From External C	Authentication			
	HPEStoreEver3040	Jun 14, 2024, 1:44:18 PM	Jun 14, 2025, 1:44:17 PM	✔ Yes	Enable			

5. Select the certificate and select the **Download** icon to download the certificate.

- 6. Unzip the downloaded file. It contains the following:
  - A certname.pem file that includes both the client certificate and private key. In this example, this file is called HPEStoreEver3040.pem.

The client certificate section of the certname.pem file includes the lines -----BEGIN CERTIFICATE----- and -----END CERTIFICATE----- and all text between them.

The private key section of the certname.pem file includes the lines -----BEGIN PRIVATE KEY----- and -----END PRIVATE KEY----- and all text in between them.

• A cacert.pem file which is the root certificate for the KMS cluster. It is always named cacert.pem.

$\leftarrow \rightarrow \land \uparrow$	> Th	s PC > Downloads > HPEStoreEver3	040_2024-06-14-19-00-00		
1.0.11		Name	Date modified	Туре	Size
🖈 Quick access	*	📄 cacert.pem	6/14/2024 2:00 PM	PEM File	5 KB
📕 Downloads	*	HPEStoreEver3040.pem	6/14/2024 2:00 PM	PEM File	2 KB

See the following link for additional information Managing KMIP Objects in the KeyControl KMIP Vault webGUI.

## 3.4. Import tenant client certificate into the StoreEver Tape Library

This resumes section Configure the KMIP server.

- 1. In the **Certificate Generation** window, select the **Keep Current Certificate** radio button this time.
- 2. In the **Signed Library Certificate**, paste the certificate created in section Create the client certificate bundle, then select **Next**.

File HPEStoreEver3040.pem contains the certificate.

Key Management Interoperability Protocol (KMIP) Wizard	Sign Library Certificate
	Sign your new certificate copied from the last page with the certificate authority you have chosen to use. Sign the
Wizard Information	certificate as a client certificate and configure the expiration duration as needed.
Certificate Authority Information	<ol> <li>Highlight the signed certificate text and copy.</li> <li>NOTE: Be sure to include the "BEGIN CERTIFICATE" and "END CERTIFICATE" lines in your copy.</li> </ol>
Certificate Authority Certificate Entry	2. Paste into box below.
	KMIP Certificate :
Library Certificate Information	BEGIN CERTIFICATE
KMIP Client Configuration	
Certificate Generation	A CONTRACTORY CONTRACTORY OF THE DECK OF T
► Sign Library Certificate	
KMIP Server Configuration	presented and a fail and conservation and also and the second second second second second
Setup Summary	
Hewlett Packard Enterprise	Back Next Finish Cancel

3. In the **KMIP Server Configuration** window, enter the IP of the Entrust KeyControl KMIP server nodes. Select **Connectivity Check** to test connectivity to the nodes, it should check OK, then select **Next** 

(ey Management Interoperability Protocol KMIP (KMIP) Wizard	Server Configuration	I		
Enter the Wizard Information and HPE e	KMIP server IP/hostname informati trongly recommends using only po	on. Up to ten KMIP se ont 5696.	rvens can be configured. The default	KMIP port is 56
After ente Certificate Authority Information authentica	ring in the KMIP server information stion.	п, иве the Connectivity	Check button to validate KMIP serve	er connectivity
Certificate Authority Certificate Entry	IP Address/FQ hostname:	Port:	IP Address/FQ hostname:	Port:
NODE1	10.02.02.000	5696 NODE	6:	5696
NODE2	• 20 10 10 mm	5696 NODE	7:	5696
MIP Client Configuration NODE3	1	5696 NODE	8:	5696
NODE	4	5696 NODE	9:	5696
ertificate Generation NODES	:	5696 NODE	10:	5696
Sign Library Certificate • KMIP Server Configuration Setup Summary			Con	nnectivity Chec
Hewlett Packard Enterprise			Back Next Fin	ish Cance

4. In the Setup Summary windows, select Finish, then select Exit.

Key Management Interoperability Protocol (KMIP) Wizard	Setup Summary	s are correct before submitting the conf	iguration by pressing the Finish button
Wizard Information	dient Usemame: N∕A		geranen ey preseng met men eerem
Certificate Authority Information	Tier1		
Certificate Authority Certificate Entry			
Library Certificate Information	Taak	Info	Done
	Library Certificate	Finished	$\bigcirc$
KMIP Client Configuration	KMIP Certificate	Finished	<b>Ø</b>
Certificate Generation	Connectivity Check	Finished	<b>S</b>
	KMIP Sener Settings Saved	Finished	<u> </u>
Sign Library Certificate	Store Configuration To System	Finished	<ul> <li>Image: A start of the start of</li></ul>
KMIP Server Configuration			
Setup Summary			
v Scrap Sammary			
Enterprise			Back Next Finish Exit

## 3.5. Set the default encryption mode

- 1. Log into the StoreEver webGUI using an account with Security Admin privileges.
- 2. In the **Set Default Encryption for new Partitions** section, select **KMIP (Licensed)** from the pull-down menu.
- 3. Select **Apply to all existing partitions**. Notice the change in **Set Encryption Mode per Partitions**.

HPE MSL3040 🟠	Lib. Health: 🗸 Status: Idle 04:001	31 PM 14.06.2024 User: security Logout ?
Serial #: Hostname:	Configuration > Encryption	Initial Configuration Wizard
IPv4: Firmwere: 3330	When changing certain configuration options the library will go offline to hosts. Only perform these config chan when it is acceptable for the library to conoffline	nges System 💝
CVTL: 1012.3.222	Cat Default Forward in Mode for your Destriction	Network
S Drives	Set beautrencryption mode for new Partitions. Will be used if a partition gets created:	Network Management 🛛 🕹
	KMIP (Licensed)	Drives
Empty Empty Empty	Course I Catiling	Mailslots
	Allow Administrator emprotion configuration during Expert Partition Witard	Partitions 🛛
	Note: Enabling this selection allows library administrators to enable and disable encryption	Encryption 🔗
	on a per-partition basis, without needing further approval from the Security user.	USB - MSL Encryption Kit
	Set Encryption Mode per Partition	KMIP Wizard
		LTO FIPS Support Mode
<u> </u>		User Accounts 🛛 🕹
<u>ل</u>	DVP. KMIP (Licensed)	Command View TL
		Web Management
	Submit	Secure Manager

4. Select Submit.

## Chapter 4. Test the integration

Testing is done using the HPE Library and Tape Tools (L&TT). Within this tool, the Drive Performance test writes and reads data to/from the specified tape drive. The Entrust KeyControl KMIP server manages the keys for the writes and reads operations. Therefore, the entire system is tested.



This test needs a tape manually loaded in the drive(s).



This test will overwrite all data on the tape, meaning that the data will be lost.

- 1. Launch the HPE Library and Tape Tools.
- 2. In L&TT Startup, select Saved/Manual Scan, NT Miniport, Check for Backup Applications and Services, then select Continue.

	<b>Hewlett Pa</b> Enterprise	ckard
HPE L	ibrary and Tape Too	ols - Version 6.05
AUTION: Running the storage devices of features of the operation of the op	is application while ot an cause unpredictable of the storage software.	her software is accessing e results and adversely
lease stop any back xit this application.	up applications and se	rvices before continuing or
O Options		
0 Options Select the Scan mode and the Ethernet connection. C	11/0 mode. Use the default 1/0 Click on 'Help' for more informati	mode unless you specifically need on.
O Options Select the Scan mode and the Ethernet connection. C <b>Scan Mode</b>	II/O mode. Use the default I/O Click on 'Help' for more informati	mode unless you specifically need on.
0 Options Select the Scan mode and the Ethernet connection. C <b>Scan Mode</b> O Hardware Scan	II/O mode. Use the default I/O lick on 'Help' for more informati Saved/Manual Scan	mode unless you specifically need on. O Skip Device Scan
0 Options Select the Scan mode and the Ethernet connection. C <b>Scan Mode</b> O Hardware Scan <b>I/O Mode</b>	II/O mode. Use the default I/O lick on 'Help' for more informati Saved/Manual Scan	mode unless you specifically need on. O Skip Device Scan
0 Options Select the Scan mode and the Ethernet connection. C <b>Scan Mode</b> O Hardware Scan <b>I/O Mode</b> NT Miniport	II/O mode. Use the default I/O Nick on 'Help' for more informati Saved/Manual Scan Ethernet (LTO-5 or later)	mode unless you specifically need on. O Skip Device Scan Please select tape library model

3. All devices available for testing should appear in the **Detected devices** left pane.

- 4. Expand the device(s) to test in the **Detected devices** pane.
- Select a Drive of a device to test, not the actual device itself. Then select Select. Repeat until all the drives to test appear in the Select devices pane. Then select Continue.

Detected devices Libraries/Autoloaders HP MSL G3 Series (Address: HP MSL 3040 (Address: 4/0 Drive 1: HPE Ultrin HP MSL6480 (Address: 4/0.3 Drive 1: HPE Ultrin Drive 2: HPE Ultrin Drive 2: HPE Ultrin Drives	Select All >> Select All >> Select > Select All >> Cancel Select > Select devices Select devices Libraries/Autoloaders Drives Select > Sel	ess ess ess
< >	4	>

6. Wait for the scan to complete. The **By Product** tab in the left pane displays the selected drive(s).

😹 HPE Library and Tape Tools - 6.05	– 🗆 X
File View Function Options Utilities Help	
ldentity Firmware Health Test	Image: Weight of the system     Image: Weight of the system     Image: Weight of the system       Utility     Support     Frontpanel     Dev Perf     Sys Perf     Help
Identity Firmware Health Test Scan By Product By Connection Instructions Dives	Utility       Support       Frontpanel       Dev Perf       Sys Perf       Help         HPE Library and Tape Tools         The system is being scanned for devices. When scanning is complete, the device list is displayed in the left section of the screen.         Next select a device to work with. Note that:         •       Only devices with blue icons are supported         •       The address is displayed as follows:         NTT Miniport I/O mode : <port #="">/&lt;#Ba&gt;.<scsi id="" target="">.<lun>         Ethernet I/O mode : <ip address="">#<port>         •       Drives in libraries are best diagnosed by selecting the library         After selecting a device, click the appropriate toolbar button to perform the desired diagnostic function.         NOTE: If the scan fails or you do not see the expected devices listed, click the Help icon on the toolbar for more information. The help is context-sensitive and may be selected at any time to obtain information about the for sensitive and may be selected at any time to obtain information about the</port></ip></lun></scsi></port>
< >>	

7. Select a drive. Then select **DevPerf** in the toolbar. Then select **Start**.

🛃 HPE Lib File View	rary and Tape Function	e Tools - 6. Options	05 Utilities	Help								_		×
(1) Identity	101101 011101 100100 Firmware	Health	<b>V</b> Test		<u>}</u> Utility	O Support	<b>Frontpanel</b>	- 😴 Dev Perf	Sys Pe	erf	Help			
Scan By	Product By (	Connection	Instructio	ns	Driv	/e Performanc	e Test Drive I	Performance	Results					
Tape Pe The purpo drive perfo server can	erforman se of this te: ormance by c access the t	<b>ce</b> st is to me hecking ho ape drive i	asure the ow fast th	tape e		Device	trium 8-SCSI)	Progre	888	Status				
of the disk pre-loade ratios dire the tape d	< subsystem. d data with d actly from the lrive.	It works b different o memory o	y ti om of t	M d: D	/ARNING ata on th o you wi	: Running Dr ne tape and t ish to continu	ive Performan he data will be ue with the te:	ce Test will o : lost. :t?	ovenwrite	ALL				>
								Yes	N	0				
						Description	This test is run   autoloaders/libr Please go to th "Drive Performa	o measure th aries test car e "Options" t ince Test Re	ne Drive F n be run o ab to con esults'' tab	Performar Inly on the figure the to view	nce. In the ca e drives asso e various test the result.	se of ciated with th options. Go to Options	em. o the	
									St	art				

8. Acknowledge the warning. Then wait for the test to complete. Then select OK.



9. Select the Drive Performance Results tab to view the results.

😹 HPE Library and Tape Tools - 6.05	-		×
File View Function Options Utilities Help	lp		
Identity Firmware Health Test	Utility Support Frontpanel Dev Perf Sys Perf Help		
Scan By Product By Connection Instructions	Drive Performance Test Drive Performance Results		
Tape Performance This screen displays the results of the tape	Device Performance Test Started on Drive (Ultrium 8-SCSI) (Tane3)	Clear Log	,
drive performance test you have run.	Testing with 2:1 Compression Ratio Opening Tape Drive Tape3 Rewinding Tape - 4.0 GB written in 6.3 seconds at 578 MB/s (Min 574 MB/s, Max 584 MB/s) Rewinding Tape - Spinning Up - 4.0 GB read in 7.5 seconds at 535 MB/s (Min 283 MB/s, Max 600 MB/s) Rewinding Tape - Closing Tape Drive Tape3		

- 10. Sign in to the KMIP Vault with the URL and credentials from Create a KMIP Vault in the Entrust KeyControl.
- 11. Select the **Objects** tab. Notice the symmetric key created during the testing conducted above.

ENTRUST	KeyControl Vault for KMIP				HPE-StoreEver-M MSI 6480	/SL3040-	o 4	?
🚓 Home 🛛 🐡 Client Certific	ates 🗙 🚯 Objects	×						
KMIP Objects								
Filter							Action	s   <del>-</del>
UUID	Description	Initial Date	Last Change Date	Object Type	Archived	State		
All designed and the first		Jul 1, 2024, 7:02:26 PM	Jul 1, 2024, 7:02:26 PM	SymmetricKey		PRE-ACTI	VE	
4021010-0004-040-0405-0		Jul 1, 2024, 7:02:31 PM	Jul 1, 2024, 7:02:31 PM	SymmetricKey		PRE-ACTI	VE	
THE R. LEWIS CO., LANSING, MICH.		Jul 1, 2024, 7:13:51 PM	Jul 1, 2024, 7:13:51 PM	SymmetricKey		PRE-ACTI	VE	
		Jul 3, 2024, 9:50:10 AM	Jul 3, 2024, 9:50:10 AM	SymmetricKey		PRE-ACTI	VE	
R14000214-00210742		Jul 4, 2024, 11:33:43	Jul 4, 2024, 11:33:43	SymmetricKey		PRE-ACTI	VE	
5007-01-010-0-0-0200-7	L	Jul 4, 2024, 11:57:00	Jul 4, 2024, 11:57:00	SymmetricKey		PRE-ACTI	VE	

- 12. Back in the **HPE Library and Tape Tools** window, select the **By Product** tab in the left pane.
- 13. Repeat steps for additional drives.

👫 Home 🔅 Client	t Certificates 🗙 🕲 Objects	×							
KMIP Objects									
liter						Actions			
UUID	Description	Initial Date	Last Change Date	Object Type	Archived	State			
10100-00100	No. (1)	Jul 1, 2024, 7:02:26 PM	Jul 1, 2024, 7:02:26 PM	SymmetricKey		PRE-ACTIVE			
1000	NOR 20.	Jul 1, 2024, 7:02:31 PM	Jul 1, 2024, 7:02:31 PM	SymmetricKey		PRE-ACTIVE			
7004074 (dia 4738	154 B	Jul 1, 2024, 7:13:51 PM	Jul 1, 2024, 7:13:51 PM	SymmetricKey		PRE-ACTIVE			
	FR. 4	Jul 3, 2024, 9:50:10 AM	Jul 3, 2024, 9:50:10 AM	SymmetricKey		PRE-ACTIVE			
81.45245.25 (cm. 44-2	NVB.	Jul 4, 2024, 11:33:43	Jul 4, 2024, 11:33:43	SymmetricKey		PRE-ACTIVE			
	100 F	Jul 4, 2024, 11:57:00	Jul 4, 2024, 11:57:00	SymmetricKey		PRE-ACTIVE			
2010/01/08 2010 022 00		Jul 4, 2024, 12:16:01	Jul 4, 2024, 12:16:01	SymmetricKey		PRE-ACTIVE			
	Notes Tal.	Jul 4, 2024, 12:19:06	Jul 4, 2024, 12:19:06	SymmetricKey		PRE-ACTIVE			

Notice the three symmetric keys created to test the three drives above.

## Chapter 5. Integrating with an HSM

For guidance on integrating the Entrust KeyControl with a Hardware Security Module (HSM), consult with your HSM vendor. If you are using an Entrust nShield HSM, refer to the Entrust KeyControl nShield HSM Integration Guide available at Entrust documentation library.

# Chapter 6. Additional resources and related products

- 6.1. Entrust products
- 6.2. nShield product documentation